COMISSÃO NACIONAL
DE PROTECÇÃO DE DADOS

Proc. 5183/2007
Ref. 02.01
N/Of. 8681 de 20.12.2007

Exmº Senhor
Presidente da
Comissão dos Assuntos Constitucionais,
Direitos, Liberdades e Garantias
Assembleia da República
Lisboa

Junto se envia o Parecer desta Comissão relativo à Proposta de Lei nº 161/X/2ª (GOV).

O Parecer vai, dada a urgência solicitada, subscrito apenas pelo relator, mas tem também a concordância dos demais membros da Comissão.

Proceder-se-á à ratificação formal do Parecer na 1ª reunião da Comissão em 2008.

Aproveito para reiterar a V.ª Ex.ª a minha muita admiração e estima pessoal.

O Presidente

Luís Lingnau da Silveira

Anexo: Fotocópia do Parecer nº 61/2007
Cópia do Parecer nº 4/2005

amm

Rua de São Bento, 148 - 3.º — 1200-821 LISBOA — Telefone: 213 928 400 - Fax: 213 976 832
E-mail: geral@cnpd.pt Internet: http://www.cnpd.pt

COMISSÃO NACIONAL
DE PROTECÇÃO DE DADOS

Proc 5183/2007

PARECER Nº 61 /2007

I) Introdução

O Sr. Presidente da Comissão de Assuntos Constitucionais, Direitos, Liberdades e Garantias solicita parecer urgente à CNPD acerca da Proposta de Lei nº 161/X/2ª (GOV) que "*Transpõe para a ordem jurídica interna a Directiva nº 2006/24/CE, do Parlamento Europeu e do Conselho, de 15 de Março de 2006, relativa à conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações electrónicas publicamente disponíveis ou de redes públicas de comunicações*".

No âmbito da preparação da Directiva 2006/24/CE, o Grupo de Trabalho de Protecção de Dados (chamado "*Grupo de Trabalho do Artigo 29º*") formulou acerca do respectivo conteúdo um parecer fortemente crítico – o Parecer nº 4/2005, emitido em 21 de Outubro de 2005 (cuja cópia se junta, a título ilustrativo).

Este Parecer foi aprovado por unanimidade, tendo assim sido subscrito, também, pelos representantes da CNPD no mencionado órgão consultivo da Comissão Europeia.

Na versão definitiva da aludida Directiva não foram, todavia, atendidas muitas das objecções suscitadas pelo Grupo do Artº 29.

Uma vez aprovada a Directiva, cumpre, de todo o modo, transpô-la.

II) Antecedentes do processo de transposição

Esta Comissão teve já oportunidade de se pronunciar – no Parecer nº 38/07, de 16 de Julho de 2007 – sobre o inicial Anteprojecto de Proposta de Lei de transposição da Directiva em causa.

O Governo veio a elaborar novo Anteprojecto de Proposta de Lei de transposição, no qual atendeu à generalidade das observações suscitadas pela CNPD – o que esta de resto reconheceu no seu Parecer nº 47/07, de 29 de Agosto de 2007 (ratificado por Deliberação nº 39/07, de 17 de Setembro de 2007).

III) Apreciação da Proposta de Lei nº 161/X/2º

A – Na generalidade

A Proposta de Lei ora em apreciação corresponde, no essencial, ao último Anteprojecto sobre o qual esta Comissão já se pronunciou favoravelmente.

Isto, claro, sem prescindir da opinião que se formulara, a nível comunitário, durante a preparação da Directiva em questão.

Mas, correndo agora o procedimento de transposição, cumpre reiterar a propósito da Proposta de Lei em análise a opinião já apresentada, acerca do último Anteprojecto, no Parecer nº 47/07.

B) – Na especialidade

Apenas cabe, assim, emitir algumas observações pontuais, acerca de certos (poucos) aspectos específicos em que a Proposta de Lei em apreciação diverge do último Anteprojecto.

E isto, claro, cingindo-nos apenas a questões relevantes para a protecção de dados pessoais.

1) Condições técnicas relativas à protecção e segurança dos dados

Onde o último Anteprojecto determinava que as condições técnicas para a protecção e segurança dos dados poderiam ("*Podem ser...*") ser fixadas por portaria conjunta dos membros do Governo envolvidos, o nº 3 do artigo 7º da Proposta de Lei formula essa regra em termos preceptivos: "*São fixadas... etc*".

Considera-se que esta solução é sem dúvida preferível, obrigando a tal fixação e não deixando a questão em termos de certa ambiguidade (e insegurança, afinal), ao enunciá-la apenas em moldes permissivos ou facultativos.

2) A informação enquanto contraordenação

A Proposta de Lei elimina, acertadamente, a pretendida contraordenação tipificada assim na al. f) do artigo 12º, nº 1 do Anteprojecto:

"*j) A informação do respectivo titular da transmissão dos dados, efectuada nos termos da presente lei;*".

Mal se entendia, com efeito, que uma conduta assim delineada pudesse configurar uma contraordenação.

E tão-pouco seria de admitir que tal infracção pudesse consistir na "*não informação*" do titular dos dados transmitidos – pois que, em regra, no âmbito duma investigação criminal, tal informação seria inaceitável.

3) Destino do produto das coimas

Prevê-se no artigo 13º, nº 2 da Proposta que o produto das coimas reverta, em 60% para o Estado e 40% para a CNPD.

Trata-se, naturalmente, de uma opção de política legislativa.

Esta solução não coincide, de todo o modo, com o regime estabelecido, em termos gerais, na Lei de Protecção de Dados Pessoais (Lei nº 67/98, de 26 de Outubro), cujo artigo 42º determina que o produto das coimas respeitantes a contraordenações em matéria de protecção de dados pessoais reverte, em partes iguais, para o Estado e a CNPD.

4) Estatísticas

O artigo 15º da Proposta prevê que seja a CNPD (o Anteprojecto cometia essa incumbência o Instituto de Comunicações de Portugal a transmitir anualmente à Comissão das Comunidades Europeias as estatísticas sobre conservação dos dados gerados ou tratados no contexto da oferta de serviços de comunicações electrónicas publicamente disponíveis ou de uma rede pública de comunicações.

Esses elementos ser-lhe-ão remetidos pelos fornecedores de serviços de comunicações electrónicas publicamente disponíveis ou de uma rede pública de comunicações (art. 4, nº 1 e 15º, nº 2).

Não parece evidente que deva recair sobre a CNPD esta função, já que não se trata, directamente, de dados pessoais – como de resto por forma expressa se dispõe no nº 2 do artigo 15º em questão.

Isto, a menos que se tenha em vista proporcionar à CNPD uma visão geral sobre a aplicação – e, daí, acerca da justificação do respectivo regime, enquanto limitativo da protecção de dados pessoais – da legislação em referência no nosso país.

IV) Conclusões

1) Constituindo um facto a publicação da Directiva 2006/24/CE – apesar das objecções oportunamente apresentadas pelo Grupo do Art. 29 –, afigura-se correcto, no essencial, o modo como através da Proposta de Lei nº 161/X/2ª se intenta transpô-la.

   Considera-se ajustado, designadamente, o prazo anual de retenção de dados previsto, bem como a precisão que nela se faz quanto à caracterização dos crimes a que se reporta.

   Reitera-se, nessa medida, o parecer positivo emitido, na generalidade, em relação à última versão do respectivo Anteprojecto.

2) Na especialidade:

   a) Merecem acolhimento, tanto a obrigatoriedade ora prevista quanto à definição de normas técnicas, como a eliminação da menos congruente contraordenação antes consignada em relação à informação dos titulares dos dados.

b) O critério percentual de repartição dos produtos das coimas entre o Estado e a CNPD constitui, naturalmente, opção de política legislativa – embora represente derrogação ao regime geral da Lei de Protecção de Dados Pessoais.

c) A incumbência conferida à CNPD, de intermediar o envio de estatísticas para a Comissão das Comunidades Europeias não se integra, em bom rigor, nas suas atribuições próprias, já que se não reporta, por definição, a dados pessoais.

Isto, a menos que se tenha em vista proporcionar, assim, à CNPD, a possibilidade de ir avaliando a efectividade, em Portugal, de utilização do esquema instituído pela Directiva em causa.

Lisboa, 20 de Dezembro de 2007

Luís Lingnau da Silveira (Presidente e relator)

Luís Barroso

Eduardo Campos

Ana Roque

Carlos Lobo

Helena António

Vasco Almeida

Grupo de Protecção de Dados do Artigo 29.º

1868/05/PT
WP 113

Parecer de 4/2005 sobre a proposta de directiva do Parlamento Europeu e do Conselho relativa à conservação de dados tratados no contexto da oferta de serviços de comunicações electrónicas publicamente disponíveis e que altera a Directiva 2002/58/CE (COM(2005)438 final de 21 de Setembro de 2005)

Adoptado em 21 de Outubro de 2005

Este grupo de trabalho foi estabelecido pelo artigo 29.º da Directiva 95/46/CE Trata-se de um órgão consultivo europeu independente em matéria de protecção de dados e privacidade. As suas atribuições são descritas no artigo 30.º da Directiva 95/46/CE e no artigo 15.º da Directiva 2002/58/CE.

O secretariado é assegurado pela Direcção C (Justiça Civil, Direitos Fundamentais e Cidadania) da Comissão Europeia, Direcção-Geral Justiça, Liberdade e Segurança , B-1049 Bruxelas, Bélgica, Gabinete N.ºLX-46 01/43.

Sítio Internet: http://europa.eu.int/comm/justice_home/fsj/privacy/index_en.htm

RESUMO

A proposta de directiva da Comissão Europeia sobre a conservação de dados coloca-nos perante uma decisão histórica.

A conservação de dados de tráfego interfere com o direito fundamental a comunicações confidenciais que é inviolável.

Qualquer restrição a este direito fundamental tem de ser baseada numa necessidade urgente, só deve ser permitida em casos excepcionais e deve ser acompanhada das salvaguardas adequadas.

Os fornecedores de serviços de comunicações electrónicas acessíveis ao público vão ser confrontados com uma medida sem precedentes que os obrigará a armazenar milhares de dados referentes a comunicações de todos os cidadãos, para fins de investigação.

O terrorismo apresenta à nossa sociedade um desafio real e urgente. A resposta dos governos a este desafio deve contemplar de forma eficaz a necessidade de os respectivos cidadãos viverem em paz e segurança, não prejudicando, porém, os seus direitos humanos individuais, nomeadamente o direito à confidencialidade dos dados, pedra angular da nossa sociedade democrática.

A iniciativa da Comissão Europeia poderá, em última análise, dar lugar ao estabelecimento de períodos máximos de conservação mais curtos do que os previstos noutras propostas recentes.

Para o grupo de trabalho previsto pelo artigo 29.º não é líquido que a justificação para uma conservação de dados obrigatória e geral, apresentada pelas autoridades competentes dos Estados-Membros, se baseie em provas claras. Este grupo também manifesta algumas dúvidas quanto à justificação dos períodos de conservação de dados propostos no projecto de directiva.

Como mencionado supra, a justificação para toda e qualquer conservação de dados obrigatória e geral deve ser claramente demonstrada e provada. Este princípio é igualmente válido em relação aos períodos máximos aplicáveis em determinado caso. De qualquer forma, as condições em que as autoridades competentes podem conhecer e utilizar tais dados a fim de combaterem a ameaça de terrorismo devem também ser enunciadas de forma explícita.

Os objectivos de conservação de dados devem ser claramente expostos na directiva no contexto da luta contra o terrorismo e a criminalidade organizada, em vez de contra outras «infracções graves» indeterminadas.

Chama-se a atenção para o facto de existirem abordagens que são menos invasivas da privacidade, por exemplo, o procedimento «quick-freeze» (congelamento rápido).

O período de conservação dos dados, se existir, deve ser tão curto quanto possível e representar o limiar de conservação máximo aplicável a todos os Estados-Membros, apesar de estes poderem estabelecer períodos de conservação mais curtos. As medidas eventualmente introduzidas devem ser amplamente publicitadas.

As provas relativas à necessidade destas medidas devem ser periodicamente avaliadas. Baseadas numa avaliação periódica realizada, pelo menos, de dois em dois ou de três em três anos e que é tornada pública, as medidas previstas em matéria de conservação de dados devem ser limitadas no tempo de acordo com o conceito «sunset legislation» (legislação de vigência limitada). Considera-se adequado o período de três anos.

De qualquer modo, no quadro normativo europeu em vigor, não é possível aceitar a imposição das referidas obrigações a fornecedores de serviços de comunicação sem previamente serem estabelecidas as salvaguardas específicas adequadas.

Por fim, o grupo de trabalho previsto pelo artigo 29.º propõe que sejam consideradas vinte salvaguardas específicas, assumindo particular relevo as exigências aplicáveis aos destinatários e ao

tratamento po terior dos dados, a necessidade de autorizações e controlos, as medidas aplicáveis aos fornecedores (e serviços igualmente no que respeita à segurança e separação lógica dos dados, a determinação las categorias de dados envolvidos e respectiva actualização e a necessidade de excluir os dados relati os ao conteúdo.

O GRUPO DE PROTECÇÃO DAS PESSOAS NO QUE RESPEITA AO TRATAMENTO DE DADOS PESSOAIS

Instituído pela Directiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995,

tendo em conta os artigos 29.º e 30.º, n.º 1, alínea a), e n.º 3, da referida directiva e o artigo 15.º, n.º 3, da Directiva 2002/58/CE do Parlamento Europeu e do Conselho, de 12 de Julho de 2002,

tendo em conta o seu regulamento interno, nomeadamente os artigos 12.º e 14.º,

adoptou o seguinte parecer:

I. Antecedentes

Em 21 de Setembro passado, no âmbito das iniciativas europeias de luta contra o terrorismo e a criminalidade organizada, a Comissão Europeia apresentou uma «*Proposta de directiva relativa à conservação de dados tratados no contexto da oferta de serviços de comunicações electrónicas publicamente disponíveis e que altera a Directiva 2002/58/CE*[1]».

O assunto em questão é de grande importância para todos os cidadãos.

A liberdade e confidencialidade da correspondência e de todas as outras formas de comunicação fazem parte dos pilares das sociedades democráticas modernas. A sua inviolabilidade está consagrada em diversos instrumentos, incluindo cartas constitucionais, sendo ainda especificamente garantida pela Convenção Europeia para a Protecção dos Direitos Humanos, instrumento que constitui a base do direito comunitário.

A directiva proposta coloca-nos perante uma decisão histórica. Pretende introduzir pela primeira vez, à escala europeia, a obrigação de conservar, para fins de investigação, milhares de dados referentes às comunicações de todos os cidadãos. Actualmente, de acordo com o previsto pelo direito comunitário, tais dados não são armazenados ou são apenas conservados, a título temporário, por fornecedores de serviços de comunicações electrónicas e, neste caso, exclusivamente para efeitos contratuais.

A conservação de dados de tráfego interfere com o direito fundamental à confidencialidade das comunicações, garantido às pessoas pelo artigo 8.º da Convenção Europeia para a Protecção dos Direitos Humanos. Numa sociedade democrática, o interesse da segurança nacional pode justificar, quando tal seja necessário, uma eventual interferência a este direito fundamental. As referidas interferências podem, em última análise, manifestar-se através do registo e da identificação de todos os contactos e de todas as relações mantidos por indivíduos, assim como dos lugares em que os acontecimentos tiveram lugar e dos meios utilizados para este efeito. O Tribunal Europeu dos Direitos do Homem sublinhou igualmente que a vigilância secreta pode prejudicar ou mesmo destruir a democracia em nome da sua defesa, acrescentando que os

[1] [COM (2005) final 438], de 21.9.2005, *ainda não publicado no JO.*

Estados não podem, em nome da luta contra a espionagem e o terrorismo, adoptar toda e qualquer medida que julguem adequada[2].

Esta é a razão pela qual, qualquer restrição a este direito fundamental tem de ser baseada numa necessidade urgente, só deve ser permitida em casos excepcionais e está sujeita às salvaguardas adequadas. A conservação de dados de tráfego, nomeadamente de dados de localização, para efeitos de aplicação da lei, deve obedecer a condições rigorosas[3], designadamente deve ter lugar apenas durante um período limitado e só quando esta conservação seja necessária, adequada e proporcional numa sociedade democrática.

Os poderes de que as autoridades encarregadas de aplicar a lei dispõem na luta contra o terrorismo devem ser eficazes, mas não podem ser ilimitados ou utilizados de forma abusiva. Deve ser encontrado um equilíbrio proporcional no sentido de garantir que não estamos a prejudicar o tipo de sociedade que pretendemos proteger. Este equilíbrio é especialmente necessário quando se trata de obrigar os fornecedores de serviços de comunicação a armazenar dados de que eles próprios não precisam. Com efeito, isto pode levar, em última análise, a um controlo contínuo, generalizado e sem precedentes, de todos os tipos de comunicação e de movimentos da totalidade de cidadãos na sua vida quotidiana. Seria armazenado um volume de informação maior do que aquele que é realmente útil para a investigação de um número limitado de casos.

Deve igualmente ser tido em atenção o impacto de uma obrigação tão geral de retenção de dados em relação a algumas comunicações que suscitam questões delicadas ligadas a certas categorias de sigilo profissional e/ou de investigação, ou a certas actividades de entidades privadas, especificamente protegidas pela lei.

Por este motivo, desde há já alguns anos, a perspectiva tanto do grupo de trabalho previsto pelo artigo 29.° como da conferência das autoridades responsáveis pela protecção dos dados tem-se afirmado de forma firme e clara. Em diversas ocasiões desde 1997, o grupo de trabalho previsto pelo artigo 29.°[4] e a Conferência Europeia[5] manifestaram algumas dúvidas sobre a necessidade de serem estabelecidas medidas gerais de conservação de dados.

---

[2] Klass e outros c/ Alemanha, n.° 49.

[3] Ver, por exemplo, o n.° 1 do artigo 15.° da Directiva 2002/58/CEE.

[4] Ver (todos os documentos estão disponíveis em *http://europa.eu.int/comm/internal_market/privacy*):
-**Parecer 9/2004** sobre um projecto de decisão-quadro [..] (Documento do Conselho 8958/04 de 28 de Abril de 2004). Um resumo das declarações seguintes pode ser encontrado no anexo a este parecer;
-**Parecer 1/2003** sobre o armazenamento de dados de tráfego para efeitos de facturação;
-**Parecer 5/2002** relativo à Declaração dos Comissários Europeus para a Protecção dos Dados na Conferência Internacional de Cardiff (9 a 11 de Setembro de 2002) sobre a conservação sistemática obrigatória dos dados relativos ao tráfego de telecomunicações;
-**Parecer 10/2001** sobre a necessidade de uma abordagem equilibrada na luta contra o terrorismo;
-**Parecer 4/2001** relativo ao Projecto de Convenção do Conselho da Europa sobre Cibercriminalidade;
-**Parecer 7/200** sobre a proposta de directiva do Parlamento Europeu e do Conselho relativa ao tratamento dos dados pessoais e à protecção da privacidade no sector das comunicações electrónicas, de 12 de Julho de 2000 COM (2000) 385;
-**Recomendação 3/99** relativa à conservação dos dados referentes ao tráfego, por parte dos fornecedores de serviços Internet, para efeitos de aplicação da lei;
-**Recomendação 2/99** relativa ao respeito pela privacidade no contexto da intercepção das telecomunicações;
-**Recomendação 3/97** relativa ao anonimato na Internet.

[5] Ver as declarações adoptadas em Estocolmo (Abril de 2000) e Cardiff (Abril de 2002).

II. AVALIAÇÃO PRELIMINAR E CONDIÇÕES PRÉVIAS GERAIS

1. Os dados conservados podem constituir uma ferramenta útil para os investigadores, mas as condições mencionadas supra devem ser inequivocamente demonstradas e justificadas.

Em primeiro lugar, o objectivo de uma medida deste tipo deve ser exposto muito claramente. Em segundo lugar, a justificação para a conservação de dados, com carácter obrigatório e geral, deve ser explicitamente demonstrada e provada. Este princípio também se aplica em relação aos períodos máximos a respeitar. Em terceiro lugar, as condições em que as autoridades competentes podem conhecer e utilizar tais dados a fim de combaterem a ameaça de terrorismo devem ser explicadas de forma a não subsistirem dúvidas.

Estas provas devem ser avaliadas periodicamente, pelo menos, e os resultados publicados, tendo-se igualmente em atenção que a introdução de meios da vigilância geral dos cidadãos pode dar lugar a estratégias por parte do terrorismo e do crime organizado que visem impedir a utilização de determinados meios. Esta situação pode implicar a necessidade de serem desenvolvidos novos métodos de vigilância ainda mais rigorosos, iniciando-se, deste modo, uma espiral de eventuais violações dos direitos fundamentais de cidadãos, difícil de contrariar. Acresce que se corre o risco de modificar o carácter da sociedade que se está a tentar preservar.

O grupo de trabalho previsto pelo artigo 29.º reconhece que algumas condições se alteraram nas nossas sociedades, como resultado dos riscos decorrentes de ameaças terroristas, e foi informado de que alguns dados podem, por vezes, ser úteis, sendo a sua utilização justificada em determinadas investigações. Além disso, o grupo de trabalho previsto pelo artigo 29.º refere que a iniciativa da Comissão Europeia pode, em última análise, dar lugar ao estabelecimento de períodos de conservação máximos mais curtos do que os previstos no passado, situação sobre a qual o referido grupo de trabalho se manifestou desfavoravelmente – a última vez através do parecer n.º 9/2004, adoptado em 9 de Novembro de 2004, WP 99.

Contudo, as circunstâncias que justificam a conservação de dados, apesar de aparentemente decorrerem de pedidos das autoridades competentes dos Estados-Membros, não parecem basear-se em provas claras. Assim, neste fase, as condições propostas não se afiguram convincentes.

Existem outras medidas úteis a ter em conta para fins de investigação e que infringem em menor medida os direitos fundamentais dos cidadãos, por exemplo o procedimento «quick freeze» em que nem os fornecedores de comunicação nem os prestadores dos serviços da Internet são obrigados a armazenar dados de tráfego. Por exemplo, em casos justificados, as autoridades encarregadas de aplicar a lei consultam as empresas e solicitam a armazenagem de certos dados. Depois de os dados serem armazenados, as agências dispõem de algumas semanas para recolherem provas a fim de obterem uma decisão judicial. A seguir, com base na referida decisão, poderão aceder aos dados.

De qualquer forma, deve estabelecer-se claramente um período de conservação geral. Este período deve ser tão curto quanto possível e estar o mais próximo possível do período de conservação para cujos objectivos originais os prestadores dos serviços de comunicações registaram os dados.

2. A harmonização das legislações dos Estados-Membros proposta actualmente pela Comissão deve clarificar que a fixação de um período obrigatório de conservação de dados à escala europeia tem de se basear numa avaliação efectuada a nível europeu em matéria de proporcionalidade que tenha em conta tanto o carácter transnacional do crime organizado como as exigências de segurança máximas de todos os Estados-Membros.

A seguir, há que precisar que o período de conservação de dados referido na directiva deve considerar-se como o limiar máximo harmonizado aplicável a todos os Estados-Membros.

Por conseguinte, é importante sublinhar que os Estados-Membros não estabelecerão períodos de conservação de dados mais longos do que os previstos na directiva, mas podem estabelecer períodos de conservação mais curtos. Recorde-se ainda que os dados devem ser apagados no termo dos referidos períodos. Neste contexto, a actual redacção do artigo 11° do projecto de directiva não é satisfatória.

O grupo de trabalho previsto pelo artigo 29.° congratula-se com o facto de a proposta conter um artigo sobre uma avaliação (artigo 12.°) a efectuar periodicamente, pelo menos, de dois em dois anos.

Nesta avaliação há que apreciar a necessidade dos dados de tráfego utilizados pelas autoridades responsáveis pela aplicação da lei em casos específicos e identificados e nela devem participar as autoridades responsáveis pela protecção de dados. O resultado destas avaliações devem ser publicados

Contudo, a mencionada avaliação não deve ser efectuada relativamente a um período indeterminado, dado que a proposta se baseia na avaliação concreta de pressupostos e condições prévias a que a mesma faz referência. Assim, as medidas de conservação de dados previstas devem ser temporalmente limitadas de acordo com o conceito legislação «sunset». O grupo de trabalho previsto pelo artigo 29.° considerou adequado um período de três anos. Após o termo deste período, as medidas nacionais de execução que impõem a conservação de dados devem deixar de ser efectivas, sem prejuízo da possibilidade de se iniciar a análise necessária para que o Conselho e o Parlamento Europeu preparem uma nova decisão e adoptem uma nova directiva antes mesmo do termo do referido período de três anos.

No que se refere ao princípio da proporcionalidade, o grupo de trabalho previsto pelo artigo 29.° é igualmente favorável à limitação do conjunto de dados a conservar no que se refere à utilização da Internet. Por outro lado, prefere a conservação de um conjunto máximo de dados do que o estabelecimento de uma lista mínima. Em geral, os dados a conservar devem limitar-se aos recolhidos pelos fornecedores para fins técnicos e de facturação.

É indispensável delimitar o acesso aos dados e as finalidades da sua utilização, garantir que todas e quaisquer medidas gerais de conservação de dados sejam acompanhadas das salvaguardas mais rigorosas e submeter as referidas medidas a uma auditoria.

3. As salvaguardas disponíveis no quadro normativo vigente sobre protecção de dados no terceiro pilar (Directivas 95/46/CE e 2002/58/CE) devem ser especificadas de forma mais concreta no que respeita ao contexto particular da aplicação da lei de conservação de dados de tráfego. As salvaguardas especificadas são vitais para assegurar que a protecção oferecida pela Directiva 2002/58/CE, nomeadamente no que se refere ao direito relativo à confidencialidade da

utilização dos serviços de comunicações electrónicas publicamente disponíveis, não é prejudicada de forma substancial.

Além disso, na opinião do grupo de trabalho previsto pelo artigo 29.°, devem ser estabelecidas salvaguardas adequadas para as operações de tratamento de dados em sectores que actualmente não são abrangidos pelo âmbito de aplicação destas directivas.

É por esta razão que o grupo de trabalho previsto pelo artigo 29.° defende, designadamente, que o próprio projecto de directiva preveja estas salvaguardas ou seja avaliado e adoptado conjuntamente com outros instrumentos jurídicos adequados. Em especial, o grupo de trabalho previsto pelo artigo 29.° considera que a «decisão-quadro relativa à protecção dos dados pessoais tratados no âmbito da cooperação policial e judiciária em matéria penal» deve ser cuidadosamente avaliada neste contexto também.

Por fim, tendo em conta a sua repercussão no âmbito dos direitos fundamentais e liberdades dos cidadãos em causa, o grupo de trabalho previsto pelo artigo 29.° julga que as medidas que venham a ser introduzidas devem ser amplamente publicitadas.

III. OUTRAS SALVAGUARDAS ESPECÍFICAS

Além do já referido, o grupo de trabalho previsto pelo artigo 29.° considera que devem ser tratadas, pelo menos, as seguintes questões:

1. FINALIDADE

Os dados só devem ser conservados com o fim específico de lutar contra o terrorismo e o crime organizado, em vez de contra quaisquer outras «infracções graves» indeterminadas. A restrição desta finalidade também deve figurar no título da directiva proposta.

2. DESTINATÁRIOS

A directiva deve estabelecer que as autoridades responsáveis pela aplicação da lei especificamente designadas só poderão aceder aos dados quando tal seja necessário para a investigação, detecção, repressão e/ou prevenção do terrorismo. Deve ser publicada a lista destas autoridades.

3. EXTRACÇÃO DE DADOS

A prevenção do terrorismo não deve incluir a extracção de dados em grande escala com base na informação referida na directiva no que se refere aos hábitos de deslocações e comunicações de pessoas sobre as quais não recaia nenhuma suspeita da autoridade de aplicação da lei. O acesso deve ser limitado aos dados necessários no contexto da investigação específica.

4. TRATAMENTO POSTERIOR

Qualquer outro tratamento dos dados conservados pelas autoridades responsáveis pela aplicação da lei para outros processos conexos deve ser regulado ou limitado de forma rigorosa através do estabelecimento de salvaguardas específicas; deverá também ser impedido todo e qualquer acesso aos dados por outras entidades públicas. A aplicação das normas definidas em anteriores instrumentos jurídicos europeus que digam respeito ao sector das comunicações electrónicas não pode ser contrária a este princípio.

5. REGISTOS DE ACESSO

Todo e qualquer acesso aos dados deve ser registado. Os registos só devem poder ser consultados, mediante pedido, pela autoridade e/ou entidade mencionadas no n.º 6 (infra), assim como pelas autoridades responsáveis pela protecção dos dados, para efeitos de controlo, e têm de ser apagados um ano após a sua criação.

6. EXAME JUDICIAL/ INDEPENDENTE

O acesso a dados deve, em princípio, ser devidamente autorizado, caso a caso, por uma autoridade judicial, sem prejuízo dos países onde haja uma possibilidade de acesso específica autorizada por lei; o acesso a dados está sujeito a controlo independente. Quando se afigure necessário, as autorizações devem especificar os dados particulares exigidos relativamente a cada caso concreto.

7.D ESTINATÁRIOS

A directiva deve indicar de forma clara os fornecedores de serviços de comunicações acessíveis ao público que se encontrem abrangidos pelas obrigações. No caso da Internet, há que estabelecer uma limitação em relação ao fornecedor de acesso e à comunicação de pessoa a pessoa (serviços de correio electrónico e comunicação vocal através do Protocolo Internet).

8. IDENTIFICAÇÃO

Julga-se ainda ser importante clarificar na presente directiva que não existe nenhuma obrigação de identificação em casos em que esta não seja necessária para efeitos de facturação ou para outros efeitos em cumprimento do contrato.

9.F INS DI ORDEM PÚBLICA

Não deve ser permitido que os fornecedores de serviços de comunicações electrónicas ou de redes tratem para fins próprios os dados conservados apenas por razões de ordem pública.

10. SEPARAÇÃO DE SISTEMAS

Em especial, os sistemas para armazenagem de dados por razões de ordem pública devem estar logicamente separados dos sistemas que os fornecedores utilizam por razões comerciais e devem ser protegidos por medidas de segurança mais rigorosas (por exemplo através tecnologias da cifragem) a fim de impedirem o acesso e utilização não autorizados.

11. MEDIDAS DE SEGURANÇA

As medidas comunitárias devem prever normas mínimas relativas a medidas técnicas e organizativas que devem ser adoptadas pelos fornecedores e definir os requisitos gerais respeitantes às medidas de segurança estabelecidas pela Directiva 2002/58/CE.

12. TERCEIROS

As medidas comunitárias devem determinar que o acesso de terceiros a dados conservados é ilegítimo.

13. DEFINIÇÕES

Deve prever-se uma definição clara das diferentes categorias de dados, assim como uma limitação dos dados de tráfego.

14. LISTA DE DADOS E MECANISMOS PARA A SUA REVISÃO

É necessário que a directiva especifique expressamente a lista de dados pessoais a conservar. Isto é importante para uma avaliação correcta da repercussão desta obrigação sobre os direitos fundamentais e as liberdades dos cidadãos em causa, devendo ter-se em atenção os riscos na sua

esfera pessoal e a as questões relacionadas com a garantia da exactidão e actualização dos dados conservados. Qualquer proposta de alteração da lista dos tipos de dados a conservar deve ser submetida à prova rigorosa da sua necessidade. Tendo em conta o impacto destas medidas nos direitos fundamentais e nas liberdades dos cidadãos, a revisão da referida lista só deve ser realizada com a aprovação do Parlamento Europeu e com a participação das autoridades responsáveis pela protecção de dados. Também deve prever-se a participação de representantes das associações de consumidores e utilizadores, das outras entidades não-governamentais relevantes e das associações europeias do sector das comunicações electrónicas. Nesta perspectiva, não parece adequado efectuar a revisão da referida lista apenas de acordo com o procedimento de comitologia, como previsto pela directiva.

15. EXCLUSÃO DE DADOS RELATIVOS AO CONTEÚDO

Uma vez que o âmbito da proposta deve excluir conteúdos de comunicações, devem ser introduzidas garantias específicas que permitam uma distinção rigorosa e eficaz entre dados relativos a conteúdos e dados de tráfego – tanto para a Internet (ou seja, apenas dados de entrada/saída de uma sessão ou outras informações, nomeadamente registos de servidores de correio, registos de «web cache» e registos de fluxo de IP) como para a telefonia (chamada em conferência, fax, serviço de mensagens curtas [SMS], voz).

16. TENTATIVAS DE COMUNICAÇÃO MAL SUCEDIDAS

As diferentes categorias de dados de tráfego relacionados com tentativas de comunicação mal sucedidas não devem ser incluídas quando não exista uma avaliação circunstanciada da adequação destas medidas à luz dos princípios mencionados supra.

17. DADOS DE LOCALIZAÇÃO

O armazenamento de dados sobre a localização não deve ir além da identificação da célula (Cell ID) no início de uma comunicação.

18. SUPERVISÃO EFECTIVA

É necessário estabelecer controlos efectivos sobre a utilização original e qualquer outra utilização compatível (incluindo duplicação) pelas autoridades judiciais no âmbito e para efeitos de um processo penal e, no que diz respeito à protecção dos dados independentemente de um processo judicial, pelas autoridades responsáveis pela protecção dos dados.

19. PUBLICIDADE

Esta directiva deve prever a obrigação de informar adequadamente todos os cidadãos no que se refere a todas e quaisquer operações de tratamento que possam ser efectuadas após a aplicação das medidas previstas neste texto legal.

20. CUSTOS

O grupo de trabalho previsto pelo artigo 29.º observa que os custos adicionais que recaem sobre fornecedores de serviços de comunicações electrónicas ou de uma rede pública de comunicações devem ser compensados pelos Estados-Membros. Este grupo de trabalho gostaria sublinhar a importância desta questão exclusivamente no que se refere às características que estão directamente relacionadas com a protecção dos dados. As medidas de conservação de dados devem igualmente incluir o reembolso dos investimentos efectuados para a adaptação dos sistemas de comunicação, dos gastos relativos à divulgação dos dados a autoridades responsáveis pela aplicação da lei e dos gastos com medidas de segurança. É preciso adoptar uma perspectiva global para prevenir quaisquer efeitos negativos tanto no que respeita à protecção de dados como em relação à esfera económica dos cidadãos, que poderiam ter de suportar alguns dos custos que recaem sobre os fornecedores. Neste contexto, também cabe considerar se o direito de um fornecedor ao reembolso de custos deve estar sujeito ao cumprimento das normas mínimas e deve ocorrer de acordo com uma base casuística.

O grupo de trabalho previsto pelo artigo 29.º acredita que as considerações expressas neste parecer serão devidamente tidas em conta e recorda que todas as salvaguardas mencionadas supra devem ser estabelecidas antes de as obrigações de conservação de dados serem postas em prática.

Feito em Bruxelas, em 21 de Outubro de 2005

Pelo Grupo

O Presidente

Peter Schaar